LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol (SBN 194857)
msobol@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Nicholas Diamand
ndiamand@lchb.com
Douglas I. Cuthbertson
dcuthbertson@lchb.com
Abbye R. Klamann (SBN 311112)
aklamann@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

CARNEY BATES & PULLIAM, PLLC
Hank Bates (SBN 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
519 West 7th St.
Little Rock, AR 72201
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs individually and on behalf of all others similar situated

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO/OAKLAND DIVISION

AMANDA RUSHING, and her child, L.L., on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

VIACOM INC.; VIACOM INTERNATIONAL INC.; UPSIGHT, INC.; and UNITY TECHNOLOGIES SF,

Defendants.

Case No. 3:17-cv-4492

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. This is an action brought by and on behalf parents of children[1] who, while playing online games via smart phone apps, have had their personally identifying information exfiltrated by Viacom Inc. and its partners, for future commercial exploitation, in direct violation of the federal Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506. Plaintiffs bring claims under state laws to obtain an injunction to cease these practices, sequester illegally obtained information, and damages.

II. PARTIES

Plaintiffs

2. Plaintiffs are a parent and her child who used an online gaming app via websites or online services operated by Defendants.

3. Plaintiff Amanda Rushing, and her child, "L.L," reside in San Francisco, California. Ms. Rushing brings this action on behalf of herself, L.L., and all others similarly situated. L.L. was under the age of 13 while using the gaming app Llama Spit Spit.

Defendants Viacom Inc. and Viacom International Inc. (together, "Viacom")

4. Defendant Viacom Inc. is an American multinational media conglomerate. Viacom Inc. (i) runs major media networks, including numerous television channels; (ii) produces, finances, and distributes motion pictures; and (iii) licenses, develops, and publishes consumer products and interactive media, including apps for children. Viacom Inc. developed and marketed the online gaming app used by Plaintiffs, Llama Spit Spit, and other online gaming apps used by millions of people in the United States. It is headquartered at 1515 Broadway, New York, NY 10036.

5. Defendant Viacom International Inc. is a subsidiary of Viacom Inc. and the holding company for Viacom Inc.'s intellectual property. It is the listed seller of the child-focused gaming app Llama Spit Spit and numerous other games for children on mobile platforms. These apps are often operated by Nickelodeon, a business unit of Viacom Media Networks.

[1] All references to "children" contained herein refer to persons under the age of 13 pursuant to COPPA's definition of children. *See* 16 C.F.R. § 312.2.

Viacom Media Networks, a division of Viacom International Inc., provides entertainment content and related branded products to consumers, including children. Viacom International Inc. is headquartered at 1515 Broadway, New York, NY 10036.

The SDK Defendants

6. The "SDK Defendants" – identified in paragraphs 7 and 8 below – are entities which provided their own proprietary computer code to Viacom, known as software development kits ("SDKs"), for installation and use in Viacom's gaming apps, including Llama Spit Spit. Each of the SDK Defendants named herein embedded their respective SDKs in Viacom's gaming apps, causing the transmittal of app users' personally identifying information to the SDK Defendants to facilitate subsequent behavioral advertising.

7. SDK Defendant Upsight, Inc. ("Upsight") is an American technology company headquartered at 501 Folsom Street, San Francisco, CA 94105.

8. SDK Defendant Unity Technologies SF ("Unity") is an American technology headquartered at 30 3rd Street, San Francisco, CA 94103

III. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1332 and 1367 because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which some members of the proposed Classes are citizens of a state different from some defendants.

10. This Court has personal jurisdiction over Defendants because they transact business in the United States, including in this District, have substantial aggregate contacts with the United States, including in this District, engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, and purposely availed themselves of the laws of the United States.

11. In accordance with 28 U.S.C. § 1391, venue is proper in this district because a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, Defendants transact business in this District, and both SDK Defendants reside in this District.

IV. INTRADISTRICT ASSIGNMENT

12. Pursuant to Civil L.R. 3-2(c), assignment to this Division is proper because a substantial part of the conduct which give rise to Plaintiffs' claims occurred in this Division. Defendants market their products throughout the United States, including in San Francisco and Alameda counties. In addition, both SDK Defendants are headquartered in San Francisco. This complaint also involves overlapping parties and substantially similar property, transactions, and events as two other complaints filed in this Division. *See McDonald et al. v. Kiloo ApS et al.*, Case No. 3:17-cv-4344 (filed Aug. 6, 2017); *Rushing et al. v. The Walt Disney Company et al.*, Case No. 3:17-cv-04419 (filed Aug. 3, 2017).

V. ALLEGATIONS APPLICABLE TO ALL COUNTS

A. The Programming of Mobile Online Gaming Apps Enables the Collection of Personal Data.

13. The number of Americans using and relying on mobile devices connected to the internet ("smart" phones, tablets, and other devices) had increased to 77% of Americans by November 2016. Consumers increasingly use smart devices to play their favorite online games, or "apps." Many apps are aimed at children, who increasingly use smart devices to play their favorite games.

14. Most consumers, including parents of children consumers, do not know that apps created for children are engineered to surreptitiously and unlawfully collect the child-users' personal information, and then exfiltrate that information off the smart device for advertising and other commercial purposes.

15. App developers contract with third-parties for the right to embed third-party computer code into the developers' apps, for various purposes. For example, a developer may incorporate Google's "In-App Billing SDK," so that app users may make purchases and payments directly to the developer. In this way, app developers are like vehicle manufacturers, which also incorporate third-party components, such as airbags or brake pads, into their vehicles, rather than develop their own component parts from scratch.

16. Advertising-specific SDKs are blocks of computer code which operate to secretly collect an app user's personal information and track online behavior to facilitate behavioral advertising or marketing analysis. In the case of an advertising SDK, the creator of the SDK will embed its SDK code into the underlying code of the app itself, collect personal information to serve behavioral advertisements, and then pay the app developer based on the number of ads shown. This practice is a substantial source of many app developers' revenue, enabling app developers to allow users to download the apps without charging a purchase price.[2]

17. App developers and their SDK-providing partners can track children's behavior while they play online games with their mobile devices by obtaining critical pieces of data from the mobile devices, including "persistent identifiers," typically a unique number linked to a specific mobile device (*e.g.*, an individual's smart phone may be identified as "45 125792 45513 7"). SDK providers, such as the SDK Defendants, use their advertising SDKs, embedded into an app in conjunction with an app developer, such as Viacom, to capture and collect persistent identifiers associated with a particular child user from her mobile device. These persistent identifiers allow SDK providers to detect a child's activity across multiple apps and platforms on the internet, and across different devices, effectively providing a full chronology of the child's actions across devices and apps. This information is then sold to various third-parties who sell targeted online advertising.

18. Key digital privacy and consumer groups described why and how a persistent identifier alone facilitates behavioral advertising:

> With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled game consoles, which are increasingly associated with individual users, rather than families. This means that marketers do not need to know the name, address, or email of a

[2] "Only 33% of US Mobile Users Will Pay for Apps This Year," eMarketer (Feb. 5, 2015), *available at* https://www.emarketer.com/Article/Only-33-of-US-Mobile-Users-Will-Pay-Apps-This-Year/1011965 (last visited August 7, 2017) ("Put a dollar sign in front of an app, and the number of people who are willing to download and install it drops dramatically. According to a new forecast from eMarketer, 80.1 million US consumers will pay for mobile apps at least once this year, representing only 33.3% of all mobile users.").

user in order to identify, target and contact that particular user.

See Comments of The Center for Digital Democracy, et al., U.S. Federal Trade Commission, *In the Matter of Children's Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

19. In other words, the ability to serve behavioral advertisements to a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (email addresses, etc.), but instead on the surreptitious collection of persistent identifiers, which are used in conjunction with other data points to build robust online profiles. Permitting technology companies to obtain persistent identifiers associated with children exposes them to the behavioral advertising (as well as other privacy violations) that COPPA was designed to prevent.

20. When children are tracked over time and across the internet, various activities are linked to a unique and persistent identifier to construct a profile of the user of a given smart device. Viewed in isolation, a persistent identifier is merely a string of numbers uniquely identifying a user, but when linked to other data points about the same user, such as app usage, geographic location (including likely domicile), and internet navigation, it discloses a personal profile that can be exploited in a commercial context. The chain of events typically works as follows: an app developer installs an SDK in an app, which collects persistent identifiers, permitting the SDK entity to sell the child's persistent identifier to an advertising network or third-party data aggregator (who then further resells the data to additional partners). An "Ad Network" will store the persistent identifiers on its servers. Later, other app or SDK developers sell that same child's persistent identifier to the Ad Network, bolstering the Ad Network's profile of the child, increasing the value of the child's data and, relatedly, the ability to serve a more highly-targeted ad to a specific device. Multiple Ad Networks or other third-parties can then buy and sell data, exchanging databases amongst themselves, creating an increasingly sophisticated and merchantable profile of how, when, and why a child uses her mobile device, along with all of the demographic and psychographic inferences that can be drawn therefrom.

21. The Ad Networks, informed by the surreptitious collection of data from children, will assist in the sale of advertising placed within the gaming apps and targeted specifically to children.

22. In sum, children's personal information is captured from them, as is information of their online behavior, which is then sold to third-parties who track multiple data points associated with a personal identifier, analyzed with the sophisticated algorithms of Big Data to create a user profile, and then used to serve behavioral advertising to children whose profile fits a set of demographic and behavioral traits.

B. COPPA Outlaws the Collection of Children's Personal Information Without Verifiable Parental Consent.

23. Children are especially vulnerable to online tracking and the resulting behavioral advertising. As children's cognitive abilities still are developing, they have limited understanding or awareness of sophisticated advertising and therefore are less likely than adults to distinguish between the actual content of online gaming apps and the advertising content that is targeted to them alongside it. Thus, children may engage with advertising content without realizing they are doing so. *See* Comments of The Center for Digital Democracy, et al., U.S. Federal Trade Commission, *In the Matter of Children's Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

24. Recognizing the vulnerability of children in the internet age, in 1999 Congress enacted COPPA. *See* 15 U.S.C. §§ 6501–6506. COPPA's express goal is to protect children's privacy while they are connected to the internet.[3] Under COPPA, developers of child-focused apps, and any third-parties working with these app developers, cannot lawfully obtain the personal information of children under 13 years of age without first obtaining verifiable consent from their parents.

25. COPPA applies to any operator of a commercial website or online service (including an app) that is directed to children and that: (a) collects, uses, and/or discloses personal information from children, or (b) on whose behalf such information is collected or maintained. Under COPPA, personal information is "collected or maintained on behalf of an operator when .

[3] *See* Federal Trade Commission, "New Rule Will Protect Privacy of Children Online," Oct. 20, 1999, *available at* https://www.ftc.gov/news-events/press-releases/1999/10/new-rule-will-protect-privacy-children-online (last visited August 7, 2017).

. . [t]he operator benefits by allowing another person to collect personal information directly from users of" an online service. 16 C.F.R. § 312.2. In addition, COPPA applies to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children.

26. Under COPPA, "personal information" includes more commonly understood information like names, email addresses, and social security numbers, but it also includes "persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services." 16 C.F.R. § 312.2. COPPA's broad definition of "personal information" is as follows:

> "individually identifiable information about an individual collected online," which includes (1) a first and last name; (2) a physical address including street name and name of a city or town; (3) online contact information (separately defined as "an email address or any other substantially similar identifier that permits direct contact with a person online"); (4) a screen name or user name; (5) telephone number; (6) social security number; (7) a media file containing a child's image or voice; (8) geolocation information sufficient to identify street name and name of a city or town; (9) a "persistent identifier that can be used to recognize a user over time and across different Web sites or online services" (including but not limited to "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier"); and (10) any information concerning the child or the child's parents that the operator collects then combines with an identifier.

27. The U.S. Federal Trade Commission ("FTC") regards "persistent identifiers" as "personally identifiable" information that can be reasonably linked to a particular child. The FTC amended COPPA's definition of "personal information" to clarify the inclusion of persistent identifiers. *See* https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry (2016 FTC Blog post from Director of the FTC Bureau of Consumer Protection) (last visited August 7, 2017).

28. In order to lawfully collect, use, or disclose personal information, COPPA requires that an operator meet specific requirements, including *each* of the following:

i. Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what

information the website operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures as set forth in the Rule;

ii. Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents; and

iii. Obtaining verifiable parental consent prior to collecting, using, and/or disclosing personal information from children.

29. Under COPPA, "[o]btaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child. . . [r]eceives notice of the operator's personal information collection, use, and disclosure practices; and [a]uthorizes any collection, use, and/or disclosure of the personal information." 16 C.F.R. § 312.2.

30. The FTC recently clarified acceptable methods for obtaining verifiable parental consent, which include: (i) providing a consent form for parents to sign and return; (ii) requiring the use of a credit card/online payment that provides notification of each transaction; (iii) connecting to trained personnel via video conference; (iv) calling a staffed toll-free number; (v) emailing the parent soliciting a response email plus requesting follow-up information from the parent; (vi) asking knowledge-based questions; or (vii) verifying a photo ID from the parent compared to a second photo using facial recognition technology. *See* https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (last visited August 7, 2017).

C. Defendants Collect and Use Children's Personal Information Through Their Game Tracking Apps.

31. Viacom developed the mobile online gaming app Llama Spit Spit, which it has marketed since March 2017.

32. In August 2012, the Center for Digital Democracy ("CDD"), and sixteen other consumer advocacy groups, filed a complaint with the FTC asking it to investigate Viacom's

website Nick.com for violating COPPA.[4] The CDD alleged that Viacom's use of "refer-a-friend" campaigns violated COPPA by encouraging users under the age of 13 to provide Viacom with their friends' email addresses for advertising purposes, which Viacom collected without obtaining prior verifiable parental consent or providing the legally-required notice.

33. In December 2012, the CDD also filed an FTC complaint against Viacom regarding its child-focused "SpongeBob Diner Dash" app, alleging that the app asks users—including children—to provide their names, email addresses, and other personal information without obtaining prior verifiable parental consent, in violation of COPPA.[5]

34. In 2016, the New York attorney general announced – following a two-year investigation into Viacom's Nick Jr. and Nickelodeon websites titled "Operation Child Tracker" – that Viacom's websites included "tracking technology that illegally enabled third-party vendors, such as marketers or advertising companies, to track children's online activity in violation of COPPA."[6] Viacom agreed to pay a $500,000 fine—the largest penalty levied against any of targeted companies—and to undergo "comprehensive reforms" to prevent improper tracking or commercial profiling of children under the age of 13. *Id.*

35. In addition to Llama Spit Spit, Viacom has developed and marketed other gaming apps which, like Llama Spit Spit, track their users, including: Ballarina – a GAME SHAKERS App, PAW Patrol Pups to the Rescue, Teenage Mutant Ninja Turtles: Portal Power, Teenage Mutant Ninja Turtles: Brothers Unite, PAW Patrol Rescue Run, Bubble Guppies: A Grumpfish Tale, PAW Patrol Air and Sea Adventures, SpongeBob Bubble Party, Dora Appisode: Perrito's Big Surprise, Dora Appisode: Check-Up Day!, Dora Appisode: Catch That Shape Train (with Llama Spit Spit, these apps are collectively referred to as the "Game Tracking Apps"). Viacom

---

[4] *See* https://www.ftc.gov/sites/default/files/documents/public_comments/16-cfr-part-312-children%E2%80%99s-online-privacy-protection-rule-supplemental-notice-proposed-rulemaking.p104503-561789-00007%C2%A0/561789-00007-83550.pdf (last visited August 7, 2017)

[5] *See* https://www.democraticmedia.org/content/nickelodeons-mobile-spongebob-game-violates-childrens-online-privacy-protection-act-says-new (last visited August 7, 2017)

[6] *See* https://ag.ny.gov/press-release/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online (last visited August 7, 2017).

offers the Games Tracking Apps for download from Apple's App Store, Google Play Store, and/or Amazon.

36. Viacom collects and maintains personal information about the users of the Game Tracking Apps, including users under the age of 13, and permits the SDK Defendants to embed their advertising SDKS to collect those users' personal information and use that information to track those users over time and across different websites and online services.

37. Viacom has control over and responsibility for any advertising and data mining permitted by or undertaken in the Game Tracking Apps. Viacom has failed to safeguard children's personal information and ensure that third-parties' collection of data from children is lawful, in part, by allowing the SDK Defendants to embed advertising SDKs in the Game Tracking Apps directed at children.

38. Each SDK Defendant has an SDK placed in Llama Spit Spit which collects persistent identifiers to track children app users over time and across the internet. In addition to Llama Spit Spit, the other Game Tracking Apps contain SDKs that surreptitiously track child users for behavioral advertising, analytics, or both. Llama Spit Spit and the other Game Tracking Apps contain multiple SDKs, each operating independently from and in concert with one another.

39. Each SDK Defendant facilitates behavioral advertising in the mobile app space by collecting personal information about app users that enables advertisers and other third-parties to reach those users over time and across different websites and online services. Each SDK Defendant does so through its proprietary SDK embedded in Viacom's Apps – including Llama Spit Spit – which collect personal information about children under the age of 13 so that advertisers and other third-parties can target those children over time and across different websites and online services.

40. Analytics and network analysis tools have detected the persistent identifiers that each Game Tracking App accessed in real time, determined which SDKs reside in the Game Tracking Apps' code, and recorded all network traffic, including encrypted data. That documentation contains raw network data, which shows the presence of persistent identifiers and documents: (i) when the Game Tracking Apps first attempted to access persistent identifiers, (ii)

which persistent identifiers were sent from a users' device, and (iii) the SDK Defendant to which they were sent.

41. Extensive analysis conducted as to each of Viacom's Game Tracking Apps and as to each SDK Defendant found substantial evidence that each of these child-directed apps collects and uses children's persistent identifiers.

2. Viacom's Game Tracking Apps Are Directed to Children.

42. COPPA defines "children" as individuals under the age of 13. *See* 16 C.F.R. § 312.2. An app is directed to children if the "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children." *See* 16 C.F.R. § 312.2.

43. Viacom's Llama Spit Spit and the other Game Tracking Apps are directed to children under age 13.[7] For example, Llama Spit Spit is an arcade shooter game app in which "users swipe and spit to defeat enemies" in an animated "Game Shakers worlds." The app description in both Apple's App Store and Google Play states, "The Spit is on! Defeat hipster enemies as you collect coins, power-ups and crazy llama costumes, Lllama-tastic (sic) scores can land you on the leaderboard, so what are you waiting for? Get spitting!" Below is a screenshot from the game:

[7] A description of the additional Game Tracking Apps, including screenshots of the games from the Google Play Store, is appended hereto as Exhibit A.

44. In the Google Play Store, Llama Spit Spit is rated "E for everyone." In the Apple Store, it is rated as appropriate for ages 4 and up. Amazon states that it is "appropriate for most users."

45. Even if the Game Tracking Apps were not directed to children, on information and belief, Defendants have actual knowledge that they collected personal information from children. The Game Tracking Apps contain child-oriented "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children." 16 C.F.R. § 312.2.

3. The Defendants Are Operators under COPPA.

46. Each Defendant is an "operator" pursuant to COPPA. Specifically, COPPA defines an "operator," in pertinent part, as:

> any person who operates a Web site located on the Internet or an

> online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation.

16 C.F.R. § 312.2.

47. Both Viacom and the SDK Defendants operate the Game Tracking Apps entirely online. Indeed, without a connection to the internet, Plaintiffs could not have downloaded and played Llama Spit Spit.

4. Defendants Engaged in the Foregoing Acts Without Obtaining Verifiable Parental Consent.

48. Defendants collected, used, or disclosed the personal information of Plaintiff's child without notifying her parents. Viacom never obtained Plaintiff Rushing's verifiable parental consent to collect, use, or disclose her child's personal information. The SDK Defendants failed to adequately ensure that when they embedded their advertising SDKs on the Game Tracking Apps or when they collected, used, or disclosed personal information from children via their advertising SDKs on the Game Tracking Apps, that Viacom had obtained verifiable parental consent to collect, use, or disclose personal information from those children.

49. Plaintiff never knew that Defendants collected, disclosed, or used her child's personal information because Defendants at all times failed to provide Plaintiff any of the required disclosures, never sought verifiable parental consent, and never provided a mechanism by which Plaintiff could provide verifiable consent.

5. Each SDK Defendant, in Coordination with Viacom, Collects, Uses, or Discloses Children's Personal Information Within Llama Spit Spit without Verifiable Parental Consent.

50. Viacom's Llama Spit Spit app contains each of the SDK Defendant's behavioral advertising SDKs.

51. Each SDK Defendant knows or should know that it operates within Llama Spit Spit.

52. Each SDK Defendant knows or should know the age rating or suggested guidance for Llama Spit Spit listed in the Google Play Store, the Apple App Store, or Amazon, within which the SDK Defendant operates.

53. Accordingly, each SDK Defendant knows or should know that its behavioral advertising SDK is contained within Llama Spit Spit, among other child-directed apps.

54. Viacom did not inform Plaintiff, her child, or class members that the SDK Defendants' behavioral advertising SDKs are incorporated into and operate within the Game Tracking Apps, including Llama Spit Spit, to collect Plaintiff's child's and class members' personal information in the form of persistent identifiers.

55. Each SDK Defendant failed to inform the Plaintiff, her child, or class members that its behavioral advertising SDK is incorporated into and operates within Llama Spit Spit to collect Plaintiff's child's and class members' personal information in the form of persistent identifiers.

56. Viacom did not obtain verifiable parental consent to track children playing the Game Tracking Apps, including Llama Spit Spit, via persistent identifiers, over time and across different websites and online services.

57. Each SDK Defendant failed to obtain verifiable parental consent to track children playing Llama Spit Spit, via persistent identifiers, over time and across different websites and online services.

58. Each SDK Defendant systemically tracks each user of Llama Spit Spit, including users under the age of 13, over time and across different websites and online services, through its behavioral advertising SDK.

59. Each SDK Defendant does this by operating within Llama Spit Spit to collect, use, and share persistent identifiers from children who play Llama Spit Spit.

60. Accordingly, each SDK Defendant, in coordination with Viacom, collects, uses, and/or discloses the personal information of Plaintiff's child and class members under the age of

13, in the form of persistent identifiers, to track children's activity over time and across different websites and online services.

61. By affirmatively incorporating the SDK Defendants' behavioral advertising SDKs into their child-directed apps and permitting them to track children by collecting, using, or disclosing their persistent identifiers without verifiable parental consent, Viacom violated COPPA.

62. Further, each SDK Defendant knew or should have known that its SDK had been incorporated into Llama Spit Spit and that engaging in the above-described tracking and collection of children's personal information violated COPPA.

6. Viacom Engages in Substantially Similar Conduct in Its Other Game Tracking Apps by Incorporating the SDK Defendants' Behavioral Advertising SDKs into Those Game Tracking Apps.

63. Viacom's other Game Tracking Apps also contain the behavioral advertising SDKs, which operate in a substantially similar manner as in Llama Spit Spit.

64. Defendant Upsight's Upsight SDK is incorporated into the following additional Game Tracking Apps developed by Viacom: Ballarina – a GAME SHAKERS App, PAW Patrol Pups to the Rescue, Teenage Mutant Ninja Turtles: Portal Power, SpongeBob Bubble Party, Teenage Mutant Ninja Turtles: Brothers Unite, Paw Patrol Rescue Run, Dora Appisode: Perrito's Big Surprise, Dora Appisode: Check-Up Day!, Dora Appisode: Catch That Shape Train, and Paw Patrol Air and Sea Adventure.

65. Defendant Unity's Unity SDK is incorporated into the following additional Game Tracking Apps developed by Viacom: PAW Patrol Pups to the Rescue, Teenage Mutant Ninja Turtles: Portal Power, Bubble Guppies: A Grumpfish Tale, and Paw Patrol Air and Sea Adventures.

D. <u>Fraudulent Concealment and Tolling.</u>

66. The applicable statutes of limitations are tolled by virtue of Defendants' knowing and active concealment of the facts alleged above. Plaintiffs and class members were ignorant of the information essential to the pursuit of these claims, without any fault or lack of diligence on their own part.

67. At the time the action was filed, Defendants were under a duty to disclose the true character, quality, and nature of their activities to Plaintiffs and the Class and Subclass. Defendants are therefore estopped from relying on any statute of limitations.

68. Defendants' fraudulent concealment is common to the Class and Subclass.

E. Named Plaintiff Allegations

Plaintiff Amanda Rushing and Her Child, L.L.

69. On March 25, 2017, Ms. Rushing downloaded Viacom's Llama Spit Spit app onto L.L.'s device in order for her child, L.L., to play the game. L.L. thereafter frequently played Llama Spit Spit on this device on an ongoing and continuous basis.

70. On information and belief, during the time L.L. played Llama Spit Spit, one or more of the SDK Defendants had, with the permission of Viacom, embedded one or more advertising SDKs which collected, disclosed, or used personal information and persistent identifiers of L.L. Defendants did not collect L.L.'s personal information to provide support for the internal operations of Llama Spit Spit, but instead to profile L.L. for commercial gain.

71. The Defendants never asked Ms. Rushing for her verifiable parental consent – in any form or at any time – to collect, disclose, or use her child's personal information, including persistent identifiers, as required by COPPA.

72. The Defendants never provided direct notice – as required by COPPA – to Ms. Rushing regarding Defendants' practices with regard to collecting, using, and disclosing her child's personal information, or regarding the rights of Ms. Rushing or her child under COPPA, either when Ms. Rushing initially downloaded the app, or afterwards, on the app's home or landing screen.

73. Defendants' tracking and collecting of L.L.'s personal information without her verifiable parental consent is highly offensive to Ms. Rushing and constitutes an invasion of her child's privacy and of Ms. Rushing's right to protect her child from this invasion.

VI. CLASS ALLEGATIONS

74. Plaintiffs seek class certification of the Class and Subclass set forth herein pursuant to Federal Rule of Civil Procedure 23.

75. Plaintiffs seek class certification of claims for the common law privacy cause of action "Intrusion Upon Seclusion," on behalf of a multi-state class, with a class defined as follows:

> **The Multi-state Class:** all persons residing in the States of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia who are younger than the age of 13, or were younger than the age of 13 when they played the Game Tracking Apps, and their parents and/or legal guardians, from whom Defendants collected, used, or disclosed personal information without verifiable parental consent.

76. Plaintiffs seek class certification of a claim for violation of the State of California Constitution Right to Privacy on behalf of a subclass of the Multi-state Class, with a subclass defined as follows:

> **The California Subclass of the Multi-state Class:** all persons residing in the State of California who are younger than the age of 13, or were younger than the age of 13 when they played the Game Tracking Apps, and their parents and/or legal guardians, from whom Defendants collected, used, or disclosed personal information without verifiable parental consent.

77. Plaintiffs reserve the right to modify or refine the Class or Subclass definitions based upon discovery of new information and in order to accommodate any of the Court's manageability concerns.

78. Excluded from the Class and Subclass are: (a) any Judge or Magistrate Judge presiding over this action and members of their staff, as well as members of their families; (b) Defendants, Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; (c) persons who properly execute and file a timely request for exclusion from the Class or Subclass; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) counsel for Plaintiffs and Defendants; and (f) the legal representatives, successors, and assigns of any such excluded persons.

79. **Ascertainability.** The proposed Class and Subclass are readily ascertainable because they are defined using objective criteria so as to allow class members to determine if they are part of a Class or Subclass. Further, the Class and Subclass can be readily identified through records maintained by Defendants.

80. **Numerosity (Rule 23(a)(1)).** The Class and Subclass are so numerous that joinder of individual members herein is impracticable. The exact number of Class or Subclass members, as herein identified and described, is not known, but download figures indicate that the Game Tracking Apps have been downloaded hundreds of millions of times.

81. **Commonality (Rule 23(a)(2)).** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class and Subclass members, including the following:

i. Whether Viacom engaged in the activities referenced in paragraphs 31 to 73 via the Game Tracking Apps;

ii. Whether the SDK Defendants engaged in the activities referenced in paragraphs 31 to 73 via the Game Tracking Apps;

iii. Whether Defendants provided disclosure of all the activities referenced in paragraphs 31 to 73 on a website as required by COPPA;

iv. Whether Defendants directly notified parents of any of the activities referenced in paragraphs 31 to 41, 45, 48 to 65, 68 to 73;

v. Whether Defendants sought verifiable parental consent prior to engaging in any of the activities referenced in paragraphs 31 to 41, 45, 48 to 65, 68 to 73;

vi. Whether Defendants provided a process or mechanism for parents to provide verifiable parental consent prior to engaging in any of the activities referenced in paragraphs 31 to 41, 45, 48 to 65, 68 to 73;

vii. Whether Defendants received verifiable parental consent prior to engaging in any of the activities referenced in paragraphs 31 to 41, 45, 48 to 65, and 68 to 73;

viii. Whether Defendants' acts and practices complained of herein violate COPPA;

ix. Whether Defendants' acts and practices complained of herein amount to acts of intrusion upon seclusion under the law of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia;

x. Whether Defendants' conduct violated Subclass members' California constitutional Right to Privacy;

xi. Whether members of the Class and Subclass have sustained damages, and, if so, in what amount; and

xii. What is the appropriate injunctive relief to ensure Defendants no longer illegally collect children's personal information to track them over time and across different websites or online services.

82. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of members of the proposed Class and Subclass because, among other things, Plaintiffs and members of the Class and Subclass sustained similar injuries as a result of Defendants' uniform wrongful conduct and their legal claims all arise from the same events and wrongful conduct by Defendants.

83. **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately protect the interests of the proposed Class and Subclass. Plaintiffs' interests do not conflict with the interests of the Class and Subclass members and Plaintiffs have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class and Subclass.

84. **Predominance & Superiority (Rule 23(b)(3)).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class and Subclass members, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The amount of damages available to individual Plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure.

Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

85. **Final Declaratory or Injunctive Relief (Rule 23(b)(2)).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or refused to act on grounds that apply generally to the proposed Class and Subclass, making final declaratory or injunctive relief appropriate with respect to the proposed Class and Subclass as a whole.

86. **Particular Issues (Rule 23(c)(4)).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues that are common to all Class and Subclass members and are capable of class-wide resolution that will significantly advance the litigation.

VII. CLAIMS FOR RELIEF

COUNT I
Intrusion Upon Seclusion
(Brought on Behalf of the Multi-state Class)

87. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

88. Plaintiffs and Class members have reasonable expectations of privacy in their mobile devices and their online behavior, generally. Plaintiffs' and Class members' private affairs include their behavior on their mobile devices as well as any other behavior that may be monitored by the surreptitious tracking employed or otherwise enabled by the Game Tracking Apps.

89. The reasonableness of such expectations of privacy is supported by Viacom's unique position to monitor Plaintiffs' and Class members' behavior through their access to Plaintiffs' and Class members' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendants' tracking.

90. Defendants intentionally intruded on and into Plaintiffs' and Class members' solitude, seclusion, or private affairs by intentionally designing the Game Tracking Apps (as well as all SDKs identified in this Complaint) to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiffs' and Class members' activities through the monitoring technologies and activities described herein.

91. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the legislation enacted by Congress, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying the online tracking of children. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiffs and Class members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

92. Plaintiffs and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

93. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class members.

94. As a result of Defendants' actions, Plaintiffs and Class members seek injunctive relief, in the form of Defendants' cessation of tracking practices in violation of COPPA, and destruction of all personal data obtained in violation of COPPA.

95. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions – which were malicious, oppressive, willful – were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT II
California Constitutional Right to Privacy
(Brought on Behalf of the California Subclass of the Multi-state Class)

96. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

97. Plaintiffs and Subclass members have reasonable expectations of privacy in their mobile devices and their online behavior, generally. Plaintiffs' and Subclass members' private affairs include their behavior on their mobile devices as well as any other behavior that may be monitored by the surreptitious tracking employed or otherwise enabled by the Game Tracking Apps.

98. The reasonableness of such expectations of privacy is supported by Viacom's unique position to monitor Plaintiffs' and Subclass members' behavior through their access to Plaintiffs' and Subclass members' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendants' tracking.

99. Defendants intentionally intruded on and into Plaintiffs' and Subclass members' solitude, seclusion, right of privacy, or private affairs by intentionally designing the Game Tracking Apps (as well as all SDKs identified in this Complaint) to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiffs' and Subclass members' activities through the monitoring technologies and activities described herein.

100. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential information about children, constituting an egregious breach of social norms. This is evidenced by, *inter alia*, the legislation enacted by Congress, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying the online tracking of children. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Subclass members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiffs and Subclass members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

101. Plaintiffs and Subclass members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

102. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Subclass members.

103. As a result of Defendants' actions, Plaintiffs and Subclass members seek injunctive relief, in the form of Defendants' cessation of tracking practices in violation of COPPA, and destruction of all personal data obtained in violation of COPPA.

104. As a result of Defendants' actions, Plaintiffs and Subclass members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions – which were malicious, oppressive, willful – were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully request that this Court:

a) Certify this case as a class action, appoint Plaintiff Rushing as Class and Subclass representative, and appoint Plaintiffs' counsel to represent the Class and Subclass;

b) Find that Defendants' actions, as described herein, constitute: (i) breaches of the common law claim of intrusion upon seclusion in the states of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia and (2) a violation of the right to privacy under California Constitution, Article I, Section 1;

c) Enter a declaratory judgment that Defendants' actions of collecting, using, or disclosing personal information of child users without first obtaining verifiable parental consent violates COPPA;

d) Enter an order permanently enjoining Defendants from collecting, using, or disclosing personal information of child users without first obtaining verifiable parental consent;

e) Award Plaintiffs and Class and Subclass members appropriate relief, including actual and statutory damages and punitive damages, in an amount to be determined at trial;

f) Award equitable, injunctive, and declaratory relief as may be appropriate;

g) Award all costs, including experts' fees, attorneys' fees, and the costs of prosecuting this action; and

h) Grant such other legal and equitable relief as the Court may deem appropriate.

Dated: August 7, 2017

Respectfully Submitted,

/s/ Michael W. Sobol

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
ndiamand@lchb.com
Douglas I. Cuthbertson
dcuthbertson@lchb.com
Abbye R. Klamann (State Bar No. 311112)
aklamann@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
519 W. 7th St.
Little Rock, AR 72201
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs and the proposed Class

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: August 7, 2017

Respectfully Submitted,

/s/ Michael W. Sobol

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
ndiamand@lchb.com
Douglas I. Cuthbertson
dcuthbertson@lchb.com
Abbye R. Klamann (State Bar No. 31112)
aklamann@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
519 W. 7th St.
Little Rock, AR 72201
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs and the Proposed Class